

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DISH NETWORK L.L.C., et al.,

Plaintiffs,

v.

ARTURO M RAMIREZ,

Defendant.

Case No. [15-cv-04712-BLF](#)

**ORDER GRANTING PLAINTIFFS’
MOTION FOR DEFAULT JUDGMENT
AND JUDGMENT**

[Re: ECF 14]

Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C., and NagraStar LLC (collectively, “DISH Network”) have moved for the entry of default judgment against Defendant Arturo M. Ramirez (“Ramirez”). DISH Network seeks damages for Defendant’s alleged violations of the Digital Millennium Copyright Act (“DMCA”) and the Federal Communications Act (“FCA”). Mot. 1, ECF 14-1. For the reasons contained herein, DISH Network’s motion for default judgment is GRANTED.¹

I. BACKGROUND

DISH Network is a satellite broadcasting company that broadcasts, among other things, movies, sports, and general entertainment programming to customers. Compl. ¶¶ 10-11, ECF 1. DISH Network also contracts for and purchases the distribution rights for programming from providers such as network affiliates, motion picture distributors, cable networks, and sports leagues. *Id.* at ¶ 12. All the programming broadcast by DISH Network are copyrighted. *Id.* at ¶ 13. Its programming is compressed, scrambled, and transmitted to its satellites, which then relay the encrypted signal to DISH Network subscribers. *Id.* at ¶ 14. Encrypting the signal ensures that

¹ Pursuant to Civil L.R. 7-9(b), the Court VACATED the hearing scheduled for May 19, 2016.

1 only paying subscribers and purchasers obtain the copyrighted works for viewing. *Id.* at ¶¶ 13-14.

2 A DISH Network television system consists of a compatible dish antenna, receiver, smart
3 card, television, and cabling to connect the components. *Id.* at ¶ 15. Each receiver and smart card
4 has a unique serial number that DISH Network uses to activate the equipment and to ensure the
5 equipment only decrypts programming the customer is authorized to receive as part of his or her
6 subscription package and pay-per-view purchases. *Id.* at ¶ 16. Specifically, the receiver processes
7 an incoming DISH Network satellite signal by locating an encrypted part of the transmission
8 referred to as the NagraStar entitlement control message and forwards it to the smart card. *Id.* at ¶
9 18. If the subscriber is tuned to a channel that he or she is authorized to watch, the smart card uses
10 its decryption keys to unlock the message, uncovering a NagraStar control word. *Id.* The control
11 word is then transmitted back to the receiver to decrypt the DISH Network satellite signal. *Id.*

12 Various devices have appeared on the market for the purpose of illegally decrypting or
13 pirating DISH Network programming. *Id.* ¶ 20. In defense, DISH Network started to change the
14 decryption keys used to access the control words. *Id.* ¶ 22. In response, a new form of satellite
15 piracy, referred to as “control word sharing” or “Internet key sharing” (“IKS”), emerged. *Id.*

16 With IKS, once piracy software is loaded on an unauthorized receiver, the end user
17 connects the receiver to the Internet. *Id.* at ¶ 23. The Internet connection automatically updates
18 the piracy software and contacts a server that provides the necessary NagraStar control words to
19 the receiver. *Id.* The computer server, referred to as an “IKS server,” has multiple, subscribed
20 NagraStar smart cards connected to it, and thus the ability to provide valid control words. *Id.* at ¶
21 24. Access to an IKS server generally requires a valid password. *Id.* Once the IKS server is
22 accessed, control words are sent from the IKS server to the unauthorized receiver, where they are
23 used to decrypt DISH Network’s signal and view programming without paying a subscription fee.
24 *Id.*

25 One such IKS server is called NFusion Private Server (“NFPS”) and is subscription based.
26 *Id.* at ¶ 26. Members can purchase a subscription to NFPS and obtain control words to bypass
27 DISH Network’s encryption. *Id.*

28 Digital TV is a vendor that sold subscriptions to NFPS. *Id.* at ¶ 27. A subscription

1 purchased from Digital TV would include a passcode to access NFPS. *Id.* DISH Network
 2 obtained copies of Digital TV's business records pertaining to Defendant Ramirez. *Id.* These
 3 records revealed that Ramirez purchased at least 97 total subscriptions ("IKS Server Passcodes")
 4 on or about May 4, 2012, May 17, 2012, June 26, 2012, and October 26, 2012. *Id.* Each IKS
 5 Server Passcode was valid for one-year and DISH Network believes Ramirez re-sold some of the
 6 passcodes and used some of the passcodes for his own personal benefit to access DISH Network's
 7 programming. *Id.* at ¶¶ 27-29.

8 On October 12, 2015, DISH Network filed a complaint against Ramirez, alleging
 9 violations of the DMCA, FCA, and ECPA. Compl., ECF 1. On December 1, 2015, DISH
 10 Network filed a motion for entry of default judgment. ECF 12. The Clerk entered default as to
 11 Ramirez on December 4, 2015. ECF 13. On January 21, 2016, DISH Network filed a motion for
 12 default judgment by the Court as to Ramirez. ECF 14.

13 **II. LEGAL STANDARD**

14 Pursuant to Federal Rule of Civil Procedure 55(b), the Court may enter default judgment
 15 against a defendant who has failed to plead or otherwise defend an action. "The district court's
 16 decision whether to enter a default judgment is a discretionary one." *Aldabe v. Aldabe*, 616 F.2d
 17 1089, 1092 (9th Cir. 1980).

18 In exercising its discretion to enter default judgment, a district court considers seven
 19 factors set forth by the Ninth Circuit in *Eitel v. McCool*, 782 F.2d 1470, 1471-72 (9th Cir. 1986)
 20 ("Eitel factors"): (1) the possibility of prejudice to the plaintiff; (2) the merits of plaintiff's
 21 substantive claim; (3) the sufficiency of the complaint; (4) the sum of money at stake in the action;
 22 (5) the possibility of dispute concerning material facts; (6) whether default was due to excusable
 23 neglect; and (7) the strong policy underlying the Federal Rules of Civil Procedure favoring
 24 decisions on the merits. In considering these factors after a clerk's entry of default, the court takes
 25 all well-pleaded factual allegations in the complaint as true, except those with regard to damages.
 26 *Televideo Sys., Inc. v. Heidenthal*, 826 F.2d 915, 917-18 (9th Cir. 1987). The Court may, in its
 27 discretion, consider competent evidence and other papers submitted with a motion for default
 28 judgment to determine damages. *Id.*

III. DISCUSSION

A. *Eitel* Factors

i. Factor One: Possibility of Prejudice to the Plaintiffs

The first *Eitel* factor considers whether the plaintiff would suffer prejudice if default judgment is not entered. Without entry of default, DISH Network would have no other means of recourse against Ramirez for the damages caused by the alleged acts of piracy. Accordingly, the first factor favors entry of default judgment. *See, e.g., Wilamette Green Innovation Ctr., LLC v. Quartis Capital Partners*, No. 14-cv-00848, 2014 WL 5281039-JCS, at *6 (N.D. Cal. 2014) (citations omitted) (“Denying a plaintiff a means of recourse is by itself sufficient to meet the burden posed by this factor.”).

ii. Factors Two and Three: Merits of Plaintiffs’ Substantive Claims and the Sufficiency of the Complaint

The Court considers the second and third *Eitel* factors—concerning the merits of DISH Network’s substantive claims and the sufficiency of its Complaint—together because of the relatedness of the inquiries. In analyzing these factors, the Court accepts as true all well-pleaded allegations regarding liability. *See, e.g., HICA Educ. Loan Corp. v. Warne*, Case No. 11-cv-04287-LHK, 2012 WL 1156402, at *2 (N.D. Cal. April 6, 2012).

a. Violations of the DMCA

DISH Network’s first cause of action alleges a violation of section 1201(a)(2) of the DMCA which prohibits trafficking “in any product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted work];

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a [copyrighted work]; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a [copyrighted work].”

17 U.S.C. § 1201(a)(2). In order to establish liability under this section, DISH Network must establish that Ramirez violated one of the three prongs. *See* 17 U.S.C. § 1201(a)(2). Moreover, “potential lawful or fair use is not a defense to § 1201(a) when its requirements are established.”

1 *DISH Network, L.L.C. v. Sonicview USA, Inc.*, 2012 WL 1965279, at *7 (S.D. Cal. May 31, 2012)
2 (citing *Realnetworks, Inc. v. DVD Copy Control Ass'n.*, 641 F. Supp. 913, 942 (N.D. Cal. 2009)).

3 DISH Network has sufficiently alleged a claim for relief under section 1202(a). According
4 to the Complaint, IKS Server Passcodes are primarily designed and produced to circumvent DISH
5 Network's security system and access DISH Network's copyrighted works. Compl. ¶¶ 28.
6 Furthermore, they have no other commercially significant purpose or use. *Id.* at ¶ 33. DISH
7 Network also alleges Ramirez trafficked in IKS Server Passcodes by buying and re-selling them.
8 *Id.* at ¶¶ 28-29. Because each subscription is valid for 1 year and Ramirez bought 97 subscriptions
9 giving him access to 97 years of encryption circumvention technology, *id.* at ¶¶ 6-7, DISH
10 Network alleges that it is unlikely the subscriptions were purchased for personal use. *DirecTV,*
11 *Inc. v. Hendrix*, No. C-04-0370 JSW (EMC), 2005 WL 757562, at *4 (N.D. Cal. Apr. 1, 2005)
12 (the number of subscriptions purchased "supports the conclusion that these were purchased for
13 resale to others to facilitate interception of satellite transmission."). Thus, DISH Network's
14 allegations fall squarely within section 1201(a)(2).

15 b. Violations of the FCA

16 DISH Network's second cause of action alleges a violation of section 605(e)(4) of the
17 FCA. This section of the FCA is similar to section 1201(a)(2) of the DMCA and makes it
18 unlawful to import or distribute any device or equipment "knowing or having reason to know" it
19 "is primarily of assistance in the unauthorized decryption of ... direct-to-home satellite services, or
20 is intended for any other activity prohibited by subsection (a)." 47 U.S.C. § 605(e)(4). Subsection
21 (a) provides that "[n]o person not being entitled thereto shall receive or assist in receiving any
22 interstate or foreign communication by radio and use such communication ... for his own benefit
23 or for the benefit of another not entitled thereto." *Id.* § 605(a). Finally, section 605(e)(4) does not
24 apply to end-users, meaning those who use the piracy access devices for their personal use rather
25 than for sale or distribution to others. *DirecTV, Inc. v. Webb*, 545 F.3d 837, 846 (9th Cir. 2008).

26 Courts have held that DISH Network's satellite broadcasts are direct-to-home satellite
27 services for purposes of the FCA. *See, e.g., DISH Network, L.L.C. v. Sonicview USA, Inc.*, 2012
28 WL 1965279, at *8 (S.D. Cal. May 31, 2012). As previously discussed, IKS Server Passcodes are

1 primarily designed and produced to decrypt DISH Network’s satellite broadcasting signal and
 2 circumvent the access control system to view unauthorized versions of copyrighted works. DISH
 3 Network has also sufficiently alleged that Ramirez purchased and re-sold passcodes. In doing so,
 4 DISH Network relies on the fact that Ramirez purchased 97 passcodes that were each valid for one
 5 year. DISH Network alleges the sheer volume of passcodes purchased supports the conclusion
 6 that they were intended for resale. For purposes of default judgment, DISH Network has alleged
 7 sufficient facts to state a claim under section 605(e)(4) of the FCA. *See, e.g., DirecTV, Inc. v.*
 8 *Hendrix*, No. C-04-0370 JSW (EMC), 2005 WL 757562, at *4 (N.D. Cal. Apr. 1, 2005).

9 **iii. Factor Four: The Sum of Money at Stake in the Action**

10 Under the fourth *Eitel* factor, the Court considers the amount of money at stake in the
 11 litigation. *BMW of North Am., LLC v. Zahra*, Case No. 15-cv-2924-CRB, 2016 WL 215983, at *4
 12 (N.D. Cal. Jan. 19, 2016). When the amount is substantial or unreasonable, default judgment is
 13 discouraged. *Id.* The DMCA and the FCA both authorize statutory damages. For violations of the
 14 DMCA section 1201(a)(2), statutory damages for each violation are “in the sum of not less than
 15 \$200 or more than \$2,500 per act of circumvention, device, product, component, offer, or
 16 performance of service....” 17 U.S.C. § 1203(c)(3)(A). The FCA authorizes a higher range of
 17 statutory damages and for each infringing product imported or distributed, the range is \$10,000 to
 18 \$100,000 per device. 47 U.S.C. §§ 605(e)(3)(C)(i)(II).

19 DISH Network seeks \$1,000 for each NFPS subscription trafficked in by Ramirez for a
 20 total of \$97,000. This amount is slightly below the middle of the range of statutory damages
 21 allowed under the DMCA and well below the minimum statutory damages set by the FCA.
 22 Ordinarily, when a large sum of money is at stake in a default judgment, this factor weighs in
 23 favor of the defendant. *See Eitel*, 782 F.2d at 1472. But because both the FCA and DMCA
 24 authorize specific statutory damages for violations, and the district court has “wide discretion in
 25 determining the amount of statutory damages to be awarded,” the amount of money requested
 26 does not weigh against the entry of default judgment. *L.A. News Serv. v. Reuters Television Int’l,*
 27 *Ltd.*, 149 F.3d 987, 996 (9th Cir. 1998). Moreover, to the extent a damages request is
 28 disproportionate, it is not enough on its own to bar default judgment, as it may be addressed by the

1 Court in deciding what damages should be awarded, assuming that a default judgment is otherwise
2 appropriate. *Joe Hand Promotions, Inc. v. Mujadidi*, No. C-11-5570, 2012 WL 3537036, at *3
3 (N.D. Cal. Aug. 14, 2012). Accordingly, this factor does not weigh strongly against the requested
4 default judgment.

5 **iv. Factors Five and Six: The Possibility of a Factual Dispute or Excusable**
6 **Neglect**

7 Under the fifth and sixth *Eitel* factors, the Court considers whether there is the possibility
8 of a factual dispute over any material fact and whether Ramirez's failure to respond may have
9 resulted from excusable neglect. *BMW*, 2016 WL 215983 at *4. Here, DISH Network served
10 Ramirez with the complaint and motion for default judgment. ECF 11, 14-8. There is no dispute
11 of material fact because Ramirez has not responded and upon an entry of default by the Clerk, the
12 factual allegations of the complaint related to liability are taken as true. There is also nothing in
13 the record to indicate that Defendant's default is a result of excusable neglect. Both factors five
14 and six weigh in favor of granting default judgment.

15 **v. Factor Seven: Policy Favoring Decisions on the Merits**

16 Although federal policy favors decisions on the merits, Rule 55(b)(2) permits entry of
17 default judgment in situations, such as this, where a defendant refuses to litigate. *J & J Sports*
18 *Prods., Inc. v. Deleon*, No. 5:13-CV-02030, 2014 WL 121711, at *2 (N.D. Cal. Jan. 13, 2014).
19 Therefore, this general policy is outweighed by the more specific considerations in this case, and
20 the seventh *Eitel* factor weighs in favor of default.

21 **vi. Summary**

22 After considering all seven *Eitel* factors, the Court finds default judgment is warranted and
23 GRANTS Dish Network's motion for default judgment against Ramirez.

24 **B. Terms of the Judgment**

25 DISH Network seeks statutory damages for each of Defendant's 97 violations of the
26 DMCA and FCA. Mot. 7-10, ECF 14-1. The DMCA allows for statutory damages ranging from
27 \$250 to \$2,000 and the FCA allows for statutory damages ranging from \$10,000 to \$100,000. *Id.*
28 DISH Network is seeking \$1,000 per violation of the DMCA and is not seeking any statutory

1 damages for violations of the FCA. *Id.* DISH Network is also seeking a permanent injunction
2 enjoining Ramirez from trafficking in NFPS subscriptions and further circumventing the access
3 controls put in place by DISH Network. *Id.* at 10-14. DISH Network is not seeking attorney's
4 fees or costs. *Id.* at 10.

5 **1. Damages**

6 The DMCA allows a successful plaintiff to recover an award of statutory damages in lieu
7 of actual damages. 17 U.S.C. § 1203(c)(3)(A) authorizing \$200 to \$2,500 per product). The
8 Court has "wide discretion in determining the amount of statutory damages to be awarded." *L.A.*
9 *News Serv. v. Reuters Television Int'l, Ltd.*, 149 F.3d 987, 996 (9th Cir. 1998). DISH Network
10 seeks statutory damages of \$1,000 per violation. Mot. 8, ECF 14-1. Dish Network offers three
11 arguments in support of its request.

12 First, DISH Network argues that the number of IKS Server Passcodes attributed to
13 Defendant is based on limited records provided by a confidential informant and only cover 2011
14 through 2013. *Id.* DISH Network also argues that the confidential informant was not the only
15 person selling passcodes. *Id.* As a result, DISH Network suggests that Ramirez may have
16 purchased passcodes post-2013 from the confidential informant or from other persons. *Id.* The
17 Court finds DISH Network's argument that Ramirez may have violated the law on other occasions
18 is speculative. While DISH Network correctly notes that if Ramirez participated in the case,
19 DISH Network would have had the opportunity to conduct discovery and determine the extent of
20 Ramirez's violations of the DMCA and FCA, that inability to conduct discovery does not open the
21 door to conjecture and speculation. If DISH Network believes Ramirez violated the law on other
22 occasions, those allegations should be made in the complaint. As a result, this argument does not
23 serve as a basis for an increased amount of statutory damages.

24 Second, DISH Network argues that the willfulness of Ramirez's conduct and the need for
25 deterrence support an award of \$1,000 per violation. In the context of section 1201(a)(2),
26 "willful" means acting with knowledge that the product at issue is designed or used for
27 circumvention. *See Sony Computer Entm't Am., Inc. v. Filippiak*, 406 F. Supp. 2d 1068, 1075 (N.D.
28 Cal. 2005) (citing *Dolman v. Agee*, 157 F.3d 708, 715 (9th Cir. 1998)). DISH Network argues that

the large number of purchases made by Ramirez, his purchase patterns, and the limited legitimate uses of IKS Server Passcodes, Ramirez knew passcodes are designed or used for circumvention. Mot. 9, ECF 14-1. The Court agrees with Defendant's argument and finds that this argument warrants an award of statutory damages higher than the minimum.

Finally, DISH Network notes that it is not requesting any damages for Ramirez's violations of the FCA and is not requests an award of attorneys' fees and costs. Mot. 9-10, ECF 14-1. Statutory damages for violations of section 605(e)(4) are significantly higher than under the DMCA and range from \$10,000 to \$100,000 for each violation. 47 U.S.C. §§ 605(e)(3)(C)(i)(II), (e)(4). DISH Network also notes that it has successfully obtained damages under the FCA in analogous cases. Mot. 9-10, ECF 14-1 (citing *DISH Network L.L.C. v. Whitcomb*, Case No. 11-cv-0333-W(RBB), ECF 17 at 5:9-23 (S.D. Cal. July 18, 2011) (\$10,000 per violation for a total of \$14.4 million); *DISH Network L.L.C. v. Dillion*, Case No. 12-CV-00157-CAB-KSC, ECF 47 at 6:18-23 (S.D. Cal. Oct. 12, 2012) (\$100,000 per violation for a total of \$12 million); *DISH Network L.L.C. v. Cintron*, Case No. 6:12-cv-00640-GKS-KRS, ECF 30 at pp. 5-6 (M.D. Fla. Jan. 25, 2013) (\$10,000 per violation for a total of \$160,000)). In the context of DISH Network forgoing higher statutory damages under the FCA, forgoing attorneys' fees and costs, and the willfulness of Ramirez's conduct, the Court finds DISH Network's request for statutory damages of \$1,000 per violation to be appropriate. Accordingly, the Court awards DISH Network \$97,000 for Ramirez's DMCA violations.

2. Permanent Injunction

DISH Network also seeks a permanent injunction under Fed. R. Civ. P. 65 and 17 U.S.C. § 1203(b)(1). Mot. 10-14, ECF 14-1. It seeks an order enjoining Ramirez from (1) manufacturing, importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes, any other code or password used in accessing an IKS server, and any other technology or part thereof that is used in circumventing DISH Network's security system or receiving DISH Network programming without authorization; (2) circumventing or assisting others in circumventing the DISH Network security system, or receiving or assisting others in receiving DISH Network's satellite signal without authorization; and (3) testing, analyzing, reverse engineering,

manipulating, or extracting code, data, or information from DISH Network's satellite receivers, smart cards, satellite stream, or any other part or component of the DISH Network security system. *Id.* at 14.

To obtain a permanent injunction, DISH Network must demonstrate the following: "(1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." *eBay, Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006).

a. Irreparable Injury and Remedies Available at Law

"Harm resulting from lost profits and lost customer goodwill is irreparable because it is neither easily calculable, nor easily compensable and is therefore an appropriate basis for injunctive relief." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1066 (N.D. Cal. 2000). Actual loss is not required to demonstrate irreparable harm; rather, "[e]vidence of threatened loss of prospective customers or goodwill" is sufficient. *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001).

DISH Network argues that it invests millions of dollars each year in security measures. Duval Decl. ¶¶ 5-10, ECF 14-2. For example, DISH Network's most recently introduced security technology took 18 months to implement and cost more than \$100 million. *Id.* at ¶ 19. Additionally, DISH Network contends that its business reputation depends on the delivery of secured content and that piracy undermines DISH Network's contractual and prospective relationship with programming providers and customers. *Id.* at ¶ 20. Finally, DISH Network argues that its reputational harm and lost sales are inherently difficult to calculate. *Id.* The average revenue per authorized subscriber is approximately \$84 per month; however a user of an IKS Server Passcode and NFPS server could enjoy full access to DISH Network programming, including premium and pay-per-view channels, for free. *Id.* at ¶ 21. Similarly, EchoStar Technologies and NagraStar are deprived of revenues gained from the sale of equipment to DISH Network subscribers. *Id.* Because the nature and extent of DISH Network programming

unlawfully received is not known, DISH Network contends that the harm is irreparable and could not be rectified with an award of monetary damages. Mot. 12, ECF 14-1.

Irreparable harm has been found in similar cases where a defendant assisted other users to unlawfully obtain access to encrypted DISH Network programming. *See, e.g., Dish Network, L.L.C. v. SatFTA*, Case No. 08-cv-01561-JF(PSG), 2011 WL 856268, at *8 (N.D. Cal. Mar. 9, 2011); *DISH Network L.L.C. v. Whitcomb*, Case No. 11-cv-0333-W(RBB), 2011 WL 1559825, at *3 (S.D. Cal. Apr. 25, 2011) (concluding that lost profits and subscribers resulting from the sale of DISH Network piracy devices constitutes irreparable harm). Because DISH Network has adequately alleged irreparable harm from the continued piracy of their content via IKS Server Passcodes, the Court finds that the first factor is satisfied. Because of the difficulty in quantifying this harm, and the nature of its statutory illegality, the Court also finds that there are no available remedies at law and the second factor is satisfied.

b. Balance of the Hardships and Public Interest

Under the third and fourth factors for a party seeking permanent injunctive relief, when a prospective injunction would “do no more than require Defendant to comply with federal and state anti-piracy laws,” then the public has an interest in the enforcement of the statutes. *SatFTA*, 2011 WL 856268, at *8. When the injunction is tailored narrowly to prevent only the illegal conduct at issue, DISH Network is entitled to a permanent injunction. *Id.* The balance of hardships favors DISH Network, because as long as Ramirez is allowed “to help others circumvent DISH’s security system and obtain free programming, DISH continues to suffer monetary and reputational harm.” *Dillion*, 2012 WL 368214, at *4. Further, there is no evidence that Ramirez’s passcodes have any legitimate purpose. Accordingly, all four factors have been met, and permanent injunctive relief is an appropriate remedy.

IV. ORDER

For the foregoing reasons, IT IS HEREBY ORDERED that:

1. DISH Network’s motion for default judgment is GRANTED.
2. The Court further ENTERS judgment in favor of DISH Network and against Defendant

Ramirez for \$97,000.

3. The following permanent injunction is hereby ENTERED against Defendant Ramirez:

Defendant is hereby permanently enjoined from:

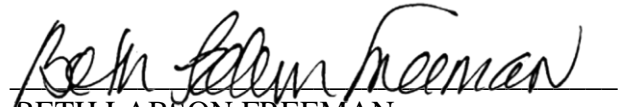
- (a) manufacturing, importing, offering to the public, providing, or otherwise trafficking in passcodes to the NFPS service, any other code or password used in accessing an IKS server, and any other technology or part thereof that is used in circumventing DISH Network's security system or receiving DISH Network programming without authorization;
- (b) circumventing or assisting others in circumventing the DISH Network security system, or receiving or assisting others in receiving DISH Network's satellite signal without authorization; and
- (c) testing, analyzing, reverse engineering, manipulating, or extracting code, data, or information from DISH Network's satellite receivers, smart cards, satellite stream, or any other part or component of the DISH Network security system.

4. The permanent injunction takes effect immediately.

5. For a district court's contempt power to apply to this injunction, Defendant Ramirez must "receive actual notice of it by personal service or otherwise." Fed. R. Civ. P. 65(d)(2). DISH Network is thus instructed to provide proper service of this order to Defendant Ramirez. DISH Network shall also file a copy of the proof of service.

IT IS SO ORDERED.

Dated: June 2, 2016


 BETH LABSON FREEMAN
 United States District Judge